Selected legal aspects of storing and access to electronic medical records

(Wybrane aspekty prawne przechowywania i dostępu do elektronicznej dokumentacji medycznej)

M Machota [1,D], J Wypyszewska [2,A,D], A Romaszewski [2,F,C], Z Kopański [2,E], M Głowacka [3,B], M Mazurek [1,B] , J Rowiński [1,B,C] , W Ptak [1,B]

Abstract – The authors discussed the principles of storing medical records. They drew attention to the specificity of legal regulations regarding storage and access to electronic medical records. They discussed the legal aspects of medical confidentiality taking into account electronic medical documents. They characterized the features of the Integrated Patient Information (ZIP) and the Patient Internet Account.

Key words – electronic medical documentation, legal aspects.

Streszczenie – Autorzy omówili zasady przechowywania dokumentacji medycznej. Zwrócili uwagę na specyfikę uregulowań prawnych dotyczących przechowywania i dostępu do elektronicznej dokumentacji medycznej. Omówili prawne aspekty tajemnicy medycznej przy uwzględnieniu elektronicznych dokumentów medycznych. Scharakteryzowali cechy Zintegrowanego Informatora Pacjenta (ZIP) oraz Internetowego Konta Pacjenta.

Słowa kluczowe – elektroniczna dokumentacja medyczna, aspekty prawne.

Author Affiliations:

1. Collegium Masoviense – College of Health Sciences, Żyrardów
2. Faculty of Health Sciences, Collegium Medicum, Jagiel-lonian University
3. Laboratory of Clinical Skills and Medical Simulation, Ludwik Rydygier Collegium Medicum in Bydgoszcz Nocolaus Copernicus University in Toruń, Poland

Authors' contributions to the article:

A. The idea and the planning of the study
B. Gathering and listing data
C. The data analysis and interpretation
D. Writing the article
E. Critical review of the article
F. Final approval of the article

Correspondence to:

Prof. Zbigniew Kopański MD PhD, Collegium Masoviense - College of Health Sciences, Żyrardów, G. Narutowicza 35 Str., PL-96-300 Żyrardów, Poland, e-mail: zkopanski@o2.pl

Accepted for publication: May 23, 2018.

I. STORAGE OF MEDICAL DOCUMENTATION

Medical records are one of the main sources of data on the patient's health status, which is the reason for the need for long-term storage. The entity preparing the internal documentation is obliged to store it, while the entity in which the service was provided stores external documentation (made in the form of referrals and orders) [1,2]. Entities preparing medical documents are obliged to store them for 20 years (from the last day of the year in which the last entry was made in the documentation). Documents must be stored for 30 years for a patient whose death has been caused by poisoning or bodily injury, and documents allowing to control the use of blood. All x-ray images not included in the documentation are stored for 10 years. Orders and referrals filled out by the doctor are stored for 5 years (if the given benefit has been granted to the patient) or 2 years (in the case it was not granted due to the absence of the patient). All documents containing data on children under the age of two are stored for 22 years. After the expiration of the required period of storage, the entities are obliged to destroy the documents or to deliver them to the patients, persons indicated by them or their representatives [3].

If the facility in which the documentation is created ceases to provide health services, it is obliged to transfer it to the acquirer, the entity creating or responsible for supervision, the entity obliged by the contract to store documents or to District Chambers: Medical or Nurses and Midwives (if documents were prepared as a part of a professional practice) [4,5]. If the documentation can not be transferred to any of the above-mentioned entities, then the voivode is responsible for its storage [3]. The District Chambers and voivode may commission another entity to process their data in a way that ensures them the ability to control their compliance and to protect the data contained in the documents [3,6].

Documentation prepared in a digital version will be kept in the SIM also after the end of the provision of health services by the entity [3,7].

Each entity storing documents must not only protect them from damage, loss and access of unauthorized persons, but also allow their sharing. This obligation also rests on every entity that takes over the documentation [3,4].

II. ACCESS TO MEDICAL DOCUMENTATION AND THE MYSTERY OF INFORMATION

There are several ways to share the documentation containing medical and personal data. The first method is to make it available for viewing in a place where a particular benefit has been provided and to allow to take photographs or notes. In this way, however, it is not possible to provide information on the rescue operations performed by EMS. Other methods of sharing the documentation are: printing, copying, and making a duplicate or abstract. The abstract is a document that contains information selected from the data contained in the medical document. The duplicate is called a document containing the text exactly rewritten from the original document, while the copy is a copy of the original by means of a photocopy or scan [3,8]. Documents may also be made available by providing their original versions (or photos taken on film), but only in the case of written confirmation of receipt and the obligation to return it. Medical documents produced in a digital version can be made available by means of electronic communication and data carriers. In addition, it is also possible to scan traditional documents [3]. There is a possibility for the entity to charge a fee for making abstracts, copies, printouts, duplicates, giving data carriers and making scans [3,8].

Medical documents about a particular patient must be shared with him. The right to process the data in the documentation is available not only to medical workers, but also to persons participating in the provision of services, responsible for maintaining teleinformation systems (in which these documents are processed) and obliged to guarantee the security of these systems. The purpose of data processing by individuals is to protect health, manage and provide benefits, as well as to guarantee the correct and safe operation of systems based on this data [3,8,9].

Entities providing health services have the right to conclude a contract with another entity, the subject of which will be the transference of data processing. The condition for the conclusion of such an agreement is to guarantee data protection and the ability of the ordering entity to check whether the data being processed is consistent with the signed contract. In addition, an order to process data from a entity other than that in which a particular service is provided can not lead to disruptions in the provision of services, and in particular can not result in restrictions on the availability of documents. If the entity receiving data from another entity ceases to process it, then it is obliged to pass it along to the ordering entity [3,6,8,9].

The institution in which the patient has received the benefit is obliged to provide her/him, the person designated by her/him or her/his representative with access to all data contained in the documentation [10,11]. In the case of a patient's death, his / her documentation may be transferred to persons indicated by him or his representative. In addition, documents containing data characterizing the patient can be made available to other entities involved in the provision of health services, which is intended to guarantee the continuation of the therapy process. Access to this documentation is also available to public authorities (such as NFZ – National Health Fund or Rzecznik Praw Pacjenta – Patient Right Ombudsman), national consultants and other entities (for the purpose of supervision and control), medical staff, health minister, representatives of the judiciary, persons involved in issuing decisions on disability or about medical events, entities whose task is to create registers, professional liability advocates, persons involved in the process of awarding quality certificates, medical committees, institutions awarding annuities, persons responsible for controlling data processing systems, as well as people who are part of teams dealing with the monitoring of infections in hospitals and heirs of the patient. The patient may also agree to share the documentation with employees of insurance companies [3,12].

Medical documents prepared by units also engaged in the training of medical personnel are obliged to provide them with access to patients' records (to the extent necessary to conduct teaching activities).

In addition, there is a possibility of transferring data for scientific purposes (to higher schools or institutes involved

in carrying out research), but only in a way that makes it impossible to determine the identity of the patient to whom the data relates [3].

Medical documents prepared in the digital version are made available according to the same criteria as traditional documents [3]. All electronic documents are made available in a way that ensures consistency and protection of data contained in them [4,13]. In the case of sharing digital documents in the form of a paper printout, the entity is obliged to appoint a person whose task will be to confirm the conformity of the data contained in the printout with the data in the electronic document. The statement of compliance must be certified with relevant information allowing this person to be identified, i.e. his/her name and surname, his/her position and his/her signature. The printout should contain data allowing identification of employees providing particular services [5].

Each entity dealing with the provision of health services is obliged to draw up a list, which contains information on patients whose documents have been made available, scope and ways of sharing them, data allowing identification of the person to whom the documentation has been passed along and the employee who made it available, as well as the date of obtaining access [3].

Every person working in the medical profession is obliged to keep all information regarding the patient confidential. This obligation applies primarily to personal and medical data. However, a medical professional may resign from this obligation if the confidentiality of the data is connected with the possibility of danger to someone's health or life or if it is necessary to provide this information to other medical employees in order to provide assistance. The third case in which employees do not have to abide the secret of information is the consent of the sick person to disclose them. The obligation of maintaining confidentiality also applies in the event of the death of the recipient. Then the person close related to him/her may agree to release the employee from the obligation of secrecy, however, this release is not valid in the case of opposition of another person close related to the deceased person [3,8,9,11].

All persons who have access to any data characterizing patients' condition are obliged to keep them secret [3].

III. INTEGRATED PATIENT INFORMATION GUIDE (ZIP) AND INTERNET PATIENT ACCOUNT (IKP)

Data included, among others, in SIM must be made available not only to medical employees, but also to patients. Currently, this access is provided, among others thanks to the ZIP, through which the patient can obtain information on health benefits reimbursed from public funds, the status of entitlements to free acquisition of services, as well as the costs of individual benefits and the location of facilities where health benefits can be obtained under health insurance. In the future, it is planned to create an IKP through which the service buyer will have access to the above-mentioned data regarding both services refunded by the NFZ and benefits financed from funds other than public funds. Therefore, IKP will provide wider access to data compared to ZIP. IKP will function as an integral element of the P1 Platform[1]. The designed account (just like ZIP) will guarantee the patient access to data characterizing the benefits provided exclusively to him. In addition, within the framework of IKP, the user will be able to submit statements about his consent for a particular benefit, transmission of medical unit data by the service provider (along with the scope of access), as well as informing other people about his health condition. An additional convenience will be the possibility of reporting, using the account by patients, the services included in the list of services provided that were not actually implemented. Users identification will be made, among others via ZIP. The integration of ZIP and IKP will guarantee the patient access to data contained in the ZIP through IKP and access to data collected in IKP via ZIP [14]. Own elaboration of the scope of data contained in ZIP and IKP is presented in Figure 1.

IV. DATE OF IMPLEMENTATION OF ELECTRONIC MEDICAL DOCUMENTATION

Medical records may be prepared and processed in a paper version by 31 December 2018. Until 31 December 2019, paper prescriptions may be written, whereas traditional versions of referral may be prepared until December 31, 2020. [15].

[1] *Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych - Electronic Platform for Collection, Analysis and Provision of Digital Resources on Medical Events*

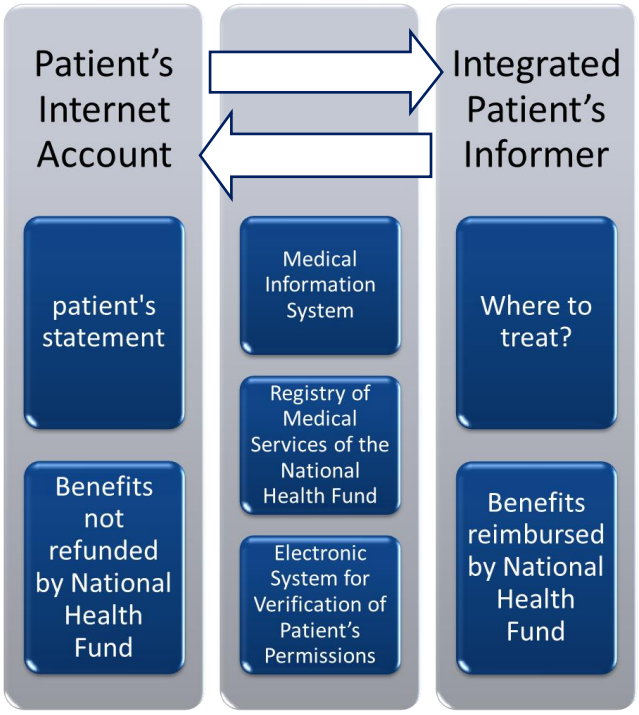

Figure 1. Own elaboration of the scope of data contained in ZIP and IKP [16]

V. REFERENCES

[1] Szymczyk D, Horoch A. Implementacja elektronicznej dokumentacji medycznej. Część 2 – korzyści dla uczestników systemu ochrony zdrowia. Med Ogólna Nauk Zdr 2013; 19(3): 324-330.

[2] Szymczyk D, Horoch A. Implementacja elektronicznej dokumentacji medycznej. Część 1 – wpływ na efektywność pracy personelu medycznego. Med Ogólna Nauk Zdr 2013; 19(3): 319-323.

[3] Ustawa z dnia 23 marca 2017 r. o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz niektórych innych ustaw (j.t. Dz. U. 2017 poz. 836).

[4] Liber A. Problemy anonimizacji dokumentów medycznych. Część 1. Wprowadzenie do anonimizacji danych medycznych. Zapewnienie ochrony danych wrażliwych metodami F(A) – I F(A,B) – anonimizacji. Puls Uczelni 2014; 8(1): 13-21.

[5] Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (j. t. Dz. U. 2015 poz. 2069).

[6] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j.t. Dz. U. 1997 nr 133 poz. 883).

[7] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (j.t. Dz. U. 2011 nr 113 poz. 657).

[8] Strzelecka A. Technologie informacyjne i komunikacyjne istotnym elementem przepływu informacji w innowacyjnej działalności podmiotów leczniczych. Zesz Nauk Polit Częstochowa 2015; 19: 44-53.

[9] Grudzińska-Kuna A, Papińska-Kacperek J. Usługi elektronicznej administracji dla obywateli w Polsce – wybrane aspekty. Rocz Kol Analiz Ekon 2012; 24: 119-131.

[10] Romaszewski A, Trąbka W. Protection of personal data in health care entities and IT systems – the impact of new, national and EU legal regulations. Zesz Nauk WSZIB Krak 2015; 37: 1-14.

[11] Romaszewski A, Trąbka W. Conditions and standards regarding medical data processing in new EU regulations. Zesz Nauk WSZIB Krak 2015; 37: 15-28.

[12] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (j.t. Dz. U. 2011 nr 113 poz. 657).

[13] Liber A. Problemy anonimizacji dokumentów medycznych. Część 2. Anonimizacja zaawansowana oraz sterowana przez posiadacza danych wrażliwych. Puls Uczelni 2014; 8(2): 13-24.

[14] Projekt ustawy o zmianie niektórych ustaw w związku z wprowadzeniem Internetowego Konta Pacjenta. Adres: https://bip.kprm.gov.pl/kpr/form/r69575821419416,Projekt-ustawy-o-zmianie-niektorych-ustaw-w-zwiazku-z-wprowadzeniem-Internetoweg.html [dostęp: 05.06.2018].

[15] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (j.t. Dz. U. 2011 nr 113 poz. 657).

[16] Projekt ustawy o zmianie niektórych ustaw w związku z wprowadzeniem Internetowego Konta Pacjenta. Adres: https://bip.kprm.gov.pl/kpr/form/r69575821419416,Projekt-ustawy-o-zmianie-niektorych-ustaw-w-zwiazku-z-wprowadzeniem-Internetoweg.html [dostęp: 05.06.2018].